

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Richard Harris

(b) County of Residence of First Listed Plaintiff Philadelphia, PA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Law Offices of Kent Petry, 1135 Mearns Road, #3387
Warminster, PA 18974. Phone: 215-322-1084

DEFENDANTS

T-Mobile, USA, Inc., et al.

County of Residence of First Listed Defendant Bellevue, Washington
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question
(U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Federal Communications Act, 47 U.S.C. §222

Brief description of cause:
Violation of the Federal Communications Act, 47 U.S.C. §222

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$
+150,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

SIGNATURE OF ATTORNEY OF RECORD

07/06/2021

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: c/o Law Offices of Kent Petry, 1135 Mearns Road #3387, Warminster, PA 18974

Address of Defendant: 12920 SE 38th Street, Bellevue, WA 98006

Place of Accident, Incident or Transaction: Philadelphia County

RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when *Yes* is answered to any of the following questions:

- | | | |
|--|------------------------------|-----------------------------|
| 1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| 4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

I certify that, to my knowledge, the within case ☐ is / ☒ is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 07/06/2021

207659

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

CIVIL: (Place a ☒ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Patent
- ☐ 6. Labor-Management Relations
- ☐ 7. Civil Rights
- ☐ 8. Habeas Corpus
- ☐ 9. Securities Act(s) Cases
- ☐ 10. Social Security Review Cases
- ☒ 11. All other Federal Question Cases

(Please specify) 47 U.S.C. §222

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury *(Please specify)* _____
- ☐ 7. Products Liability
- ☐ 8. Products Liability - Asbestos
- ☐ 9. All other Diversity Cases

(Please specify) _____

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Kent Petry, counsel of record or pro se plaintiff, do hereby certify:

☒ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: 07/06/2021

207659

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

CASE MANAGEMENT TRACK DESIGNATION FORM

RICHARD HARRIS

v.

T-MOBILE, USA, INC.

:
:
:
:
:

CIVIL ACTION

NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

- (a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ()
- (b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ()
- (c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ()
- (d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ()
- (e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) ()
- (f) Standard Management – Cases that do not fall into any one of the other tracks. (X)

7/6/21
Date

[Signature]
Attorney-at-law

PLAINTIFF
Attorney for

215-322-1084
Telephone

215-798-8054
FAX Number

kent@petrylaw.net
E-Mail Address

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

RICHARD HARRIS

Plaintiff,

v.

T-MOBILE USA, INC.; DOES 1
through 10, inclusive,

Defendant(s).

CIVIL ACTION

No.:

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff, Richard Harris (“Plaintiff”), by and through his undersigned counsel, complains against Defendant T-Mobile USA, Inc. (“T-Mobile” or “Defendant”) and Does 1 through 10, as follows:

I. INTRODUCTION

1. This action arises out of T-Mobile’s systemic and repeated failures to protect and safeguard its customers’ highly sensitive personal and financial information against common, widely reported, and foreseeable attempts to illegally obtain such information.

2. As a result of T-Mobile’s misconduct as alleged herein, including their gross negligence in protecting customer information, its negligent hiring and supervision of customer support personnel and its violations of federal and state laws designed to protect wireless service consumers, Plaintiff lost 1.63151657 bitcoin (“BTC”), with a current estimated value in excess of \$55,000, due to an account takeover scheme (also known as a “SIM-swap”) which could not have occurred but for Defendants’ intentional actions and negligent practices, as well as their repeated failure to adhere to federal and state laws.

II. **JURISDICTION AND VENUE**

3. This Court has jurisdiction of Plaintiff's claims pursuant to 28 U.S.C. §§1331, as this case arises under federal statutes, such as the Federal Communications Act ("FCA") at 47 U.S.C. §222, the Stored Communications Act ("SCA") at 18 U.S.C. §2701, and the Computer Fraud and Abuse Act ("CFAA") at 18 U.S.C. §1030.

4. This Court further has jurisdiction over this matter under 18 U.S.C. §1030(g), as this case arises under the Court's federal question jurisdiction and monetary threshold requirements pursuant to the CFAA.

5. Pursuant to the Court's supplemental jurisdiction under 28 U.S.C. §1367, it may entertain the state law claims as they are derived from a common nucleus of operative facts.

6. Furthermore, the Court has jurisdiction under 28 U.S.C. §1332 in that the amount in controversy exceeds \$75,000.00 and Plaintiff and Defendant are citizens of different states. Plaintiff is a resident of Pennsylvania, and Defendant is a Delaware corporation with a principal place of business in the State of Washington.

7. Jurisdiction is further proper in this court under the FCA pursuant to the terms of 47 U.S.C. §207.

8. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(1)-(3) upon information and belief, and because:

- a. Plaintiff is a resident of this District;
- b. The wrongful conduct was directed to and was undertaken within the territory of this District; and
- c. Defendant conducts a substantial portion of its business in this District.

III. **PARTIES**

9. Plaintiff, Richard Harris, is a male citizen of the United States of America residing in the Commonwealth of Pennsylvania and within Philadelphia County.

10. Defendant, T-Mobile, is a corporation formed under the laws of the State of Delaware, with headquarters and principal place of business in Bellevue, Washington, that serves as the American operating arm of T-Mobile International AG & Co., a corporate entity based in Germany.

11. Plaintiff is unaware of the names and capacities of those defendants sued as Does 1 through 10, but will seek leave to amend this complaint once their identities become known to Plaintiff. Upon information and belief, Plaintiff alleges that at all relevant times, each defendant, including the Doe defendants 1 through 10, was the officer, director, employee, agent, representative, alter ego, or co-conspirator of each of the other defendants, and in engaging in the conduct alleged herein was acting in the course and scope of and in furtherance of such a relationship.

12. Unless otherwise specified, Plaintiff will refer to all defendants collectively as “Defendant” and each allegation pertains to each Defendant.

13. At all times material hereto, Defendant acted and/or failed to act in person and/or through duly authorized agents, servants, workmen, and/or employees, acting within the scope and course of their authority and/or employment for and/or on behalf of Defendant.

IV. **FACTUAL BACKGROUND**

A. **GENERAL BACKGROUND**

14. T-Mobile markets and sells wireless cellular phone service through standardized wireless service plans via various retail locations, online sales, and over the telephone.

15. T-Mobile maintains accounts for its wireless customers, enabling them to access information about the services they purchase from T-Mobile.

16. It is widely recognized and has been widely publicized that mishandling of customer wireless accounts, including, but not limited to, allowing unauthorized access, can facilitate identity theft and related consumer harm.

17. Numerous instances of mishandling of customer account information have occurred at T-Mobile.

18. As one of the nation's largest wireless carriers, T-Mobile's operations must comply with various federal and state statutes, including (but not limited to) the Federal Communications Act ("FCA") 47 U.S.C. §222.

19. The FCA obligates T-Mobile to protect the "confidential proprietary information of [its] customers" and "customer proprietary network information" (commonly referred to as "CPI" and "CPNI", respectively). See 47 U.S.C. §222(a), (c).

20. The Federal Communications Commission ("FCC") has promulgated rules to implement Section 222 of the FCA "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." 1998 CPNI Order, 13 FCC Rcd. at 8195 ¶193; see also 47 C.F.R. §64.2001 *et seq.* ("CPNI Rules").

21. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. See 47 C.F.R. §64.2005.

22. The CPNI Rules also require carriers to implement safeguards to protect customers' CPNI. See 47 C.F.R. §64.2009(b), (d), and (e).

23. These safeguards include: (a) training personnel “as to when they are and are not authorized to use CPNI”; (b) establishing “a supervisory review process regarding carrier compliance with the rules”; and (c) filing annual compliance certificates with the FCC. Id.

24. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. For example, “carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.” See 47 C.F.R. §64.2010(a).

25. T-Mobile regularly holds itself out to the general public as a secure and reliable custodian of customer data, including customer’s confidential financial and personal information.

26. T-Mobile maintains that it uses a variety of “administrative, technical, contractual, and physical safeguards” to protect customers’ data against “unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control.” See <https://www.t-mobile.com/privacy-center/our-practices/privacy-policy>, as of June 2, 2021.

27. As an example, T-Mobile explicitly states that “when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access.” Id.

28. Upon information and belief, T-Mobile’s sales and marketing materials make similar representations regarding T-Mobile’s alleged implementation of various safeguards to protect its customers’ private information (as required by statutes).

29. Despite these assurances and other similar statements, T-Mobile failed to provide reasonable and appropriate security to prevent unauthorized access to customers’ accounts.

30. For instance, upon information and belief, under the inadequate procedures (if any) implemented by T-Mobile, unauthorized persons, including T-Mobile’s own officers, agents, and

employees can authenticate, access, share, and make changes to customers' information without customer permission.

31. T-Mobile failed to disclose or made deceptive statements designed to cover up for the fact that it is aware that their security procedures can and do fall short of their expressed and implied representations and promises, as well as their statutory duties.

32. Such failures, which lead to unauthorized access of customers' information, were entirely foreseeable by T-Mobile.

B. "SIM-SWAPPING" SCAM

33. As T-Mobile is aware, various forms of account takeover fraud have been widely reported in the press, by government regulators (including the Federal Trade Commission ("FTC") and the FCC), academic publications, and multiple lawsuits across the country.

34. These illegal schemes involve criminals and fraudsters gaining access to or "hijacking" customer wireless accounts, which often include sensitive personal and financial information, to induce third parties to conduct transactions with individuals they believe to be legitimate or known to them.

35. Sometimes these schemes are perpetrated by employees of the wireless carriers, such as T-Mobile.

36. One of the most damaging and pervasive forms of account takeover fraud is known as a "SIM-Swap", whereby a third-party (with the help of a wireless carrier like T-Mobile) is allowed to transfer access to a customer's cellular phone number from the customer's registered "subscriber identity module" card (or "SIM card") – to a SIM card¹ controlled by the third party.

¹ A SIM card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and to know which subscriber is associated with that phone. The SIM card associated with a wireless phone can be changed, allowing customers to move their wireless number from one cell phone to another, and to continue

37. The wireless carrier, however, must effectuate the SIM card reassignment and, therefore, “SIM-swapping” is not an isolated criminal act, as it requires the wireless carrier’s active involvement to swap the SIM containing information regarding its customer to an unauthorized person’s phone.

38. Indeed, unlike a direct hack of data, whereby a company like T-Mobile plays a more passive role, SIM-swaps are ultimately effectuated by the wireless carrier itself. For instance, in this case, it is T-Mobile that approved and allowed the SIM card change (without Plaintiff’s authorization), as well as all of the subsequent telecommunication activity that was used to access Plaintiff’s online accounts and cause the injuries suffered by Plaintiff.

39. As such, by directly or indirectly exceeding the authorized access to customer accounts, wireless carriers such as T-Mobile may be liable under state and federal statutes, such as the Federal Communications Act (“FCA”).

40. Once a third-party has access to the legitimate user’s SIM card data, it can then seamlessly impersonate that legitimate wireless customer (e.g., in communicating with others or contacting various vendors).

41. A common target of SIM-swapping and account takeover fraud are individuals known, or expected, to hold cryptocurrency, because account information is often contained on users’ cellular phones, allowing criminals to transfer the legitimate user’s cryptocurrency to an account the third-party controls.²

accessing their carrier network when they switch cell phones. The wireless carrier must effectuate the SIM card reassignment.

² Indeed, over the past year, T-Mobile has been subjected to multiple lawsuits, where as a result of SIM-swaps effectuated by T-Mobile, cryptocurrency holders have lost millions of dollars’ worth of cryptocurrency. See Kesler v. T-Mobile USA, Inc., 2:21-cv-02516-PBT (E.D.Pa.); Cheng v. T-Mobile USA, Inc., Docket No. 1:21-cv-01085 (S.D.N.Y.); Middleton, et al v. T-Mobile USA, Inc., Docket No. 1:20-cv-03276 (E.D.N.Y.).

42. SIM-swaps are not a new unforeseeable phenomenon, but instead have been discussed by federal authorities and telecommunications companies since at least 2016.

43. In June 2016, the FTC's then Chief Technologist, herself a victim of an account takeover, recounted her experience and offered advice to wireless carriers to help consumers avoid these takeover attacks, stating:

The mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts. In fact, many of them are obligated to comply with the Red Flags Rule, which, among other things, requires them to have a written identity theft prevention program.

Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions...

[M]obile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.³

44. Attention in the media and by government regulators, however, did not ensure that wireless carriers like T-Mobile took security seriously enough to prevent account takeover accounts, and SIM-swapping schemes from increasing, or to convince themselves as a company to stop engaging in practices that were clearly violative of federal law.

45. An empirical study conducted by researchers at Princeton University and publicized in early 2020 (the results of which were known to T-Mobile prior to publication)

³ Lorrie Cranor, "Your mobile phone account could be hijacked by an identity thief," Tech@FTC (June 7, 2016), available at <https://www.ftc.gov/>. Mrs. Cranor also detailed her concerns about SIM-swapping in her reply comments before the FCC in July 2016. See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket No. 16-106 (July 6, 2016).

“identified weak authentication schemes and flawed policies” at several major wireless carriers in the United States, including T-Mobile.⁴

46. The study further demonstrated that “these flaws enable[d] straightforward SIM swap attacks,” as the researchers succeeded in all ten of their attempts to effectuate a SIM-swap on T-Mobile accounts. Id.

47. This study established a clearly known vulnerability of T-Mobile’s customer authentication process(es) (the use of recent call logs) that enabled criminals to easily secure access to the personal information of T-Mobile’s customers.

48. Even before the results of the Princeton study were made available to T-Mobile, however, in May 2018, a popular information security blog, “Krebs on Security,” detailed several failures by T-Mobile to keep its customers’ data secure, including lack of adequate supervision of T-Mobile’s employees (one of whom perpetuated an account takeover scheme with knowledge of T-Mobile’s vulnerable internal systems), and failing to send legitimate customers notice to their personal e-mail when a SIM-swap occurs.⁵

49. The article pointed out that T-Mobile “also acknowledged that it does not currently send customers an email to the email address on file when SIM swaps take place. A T-Mobile spokesperson said the company was considering changing the current policy, which sends the customer a text message to alert them about the SIM swap” to the phone number that is now in the third-party’s control. Id.

⁴ Kevin Lee, et al., “An Empirical Study of Wireless Carrier Authentication for SIM Swaps,” Dept. of Comp. Sci. and Ctr. for Info. Tech. Policy, Princeton University (Jan. 10, 2020), pp. 2, 10 (discussing T-Mobile’s failures with respect to using call log verification based on the study’s research in January 2020).

⁵ Brian Krebs, “T-Mobile Employee Made Unauthorized ‘SIM Swap’ to Steal Instagram Account,” Krebs on Security (May 18, 2018), available at <https://krebsonsecurity.com/>.

50. As the blog's author concluded with regard to sending a text to a phone number that is already hijacked, "obviously that does not help someone who is the target of a SIM swap." Id.

51. In a 2019 article about SIM-swapping that included multiple quotes from T-Mobile personnel, the New York Times reported that "[c]riminals have learned how to persuade mobile phone providers like T-Mobile and AT&T to switch a phone number to a new device that is under their control."⁶

52. In February of 2020, the FCC issued a "Notice of Apparent Liability for Forfeiture and Admonishment," proposing a penalty of \$91,630,000.00 against T-Mobile for misuse of CPNI, where Commissioner Geoffrey Starks explained:

Going forward, Americans must be able to place trust in their wireless carriers....[T]hese carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just [a] few. Carriers must take responsibility for those people they allow into their operations.⁷

53. Despite the massive amounts of media, governmental, and academic focus on the issue of SIM-swaps and the internal vulnerabilities of wireless carrier systems, T-Mobile has been unable or unwilling to institute the practices, procedures, and safeguards necessary to protect its customers' data from account takeover and SIM-swap attacks.

54. Most troubling, T-Mobile has not improved its safety protocols even though it knows from numerous incidents that some of its own employees actively cooperate with hackers in SIM-swap frauds by allowing direct access to customer information and/or by ignoring or overriding T-Mobile security procedures.

⁶ Nathaniel Popper, "Hackers Hit Twitter C.E.O. in a 'SIM-swap.' You're at Risk, Too," New York Times (September 5, 2019).

⁷ In the Matter of T-Mobile USA, Inc., File No. EB-TCD-18-00027702 (February 28, 2020).

55. The prevalence of SIM-swap fraud and T-Mobile's knowledge of such fraud, including, but not limited to, that performed with the active participation of its own employees, demonstrate that what happened with Plaintiff's account was neither an isolated incident nor an unforeseeable event.

56. As a regulated wireless carrier, T-Mobile has a well-established duty – one which it freely acknowledges on its corporate website – to protect the security and privacy of CPI and CPNI from unauthorized access and T-Mobile is obligated to certify its compliance with this mandate to the FCC every year.⁸

57. The FCA expressly restricts carriers like T-Mobile from unauthorized disclosure of CPNI.

58. In light of the above, at the time of the events at issue in the present case, T-Mobile was keenly aware of its obligations, as well as multiple weaknesses in its internal processes and procedures to authenticate legitimate customers.

59. Yet T-Mobile failed to prevent the "SIM-swap" in this case (and many others), causing Plaintiff to lose approximately 1.63151657 bitcoin ("BTC"), with a current estimated value in excess of \$55,000.

C. THE "SIM-SWAP" OF PLAINTIFF'S ACCOUNT

60. In July of 2020, Plaintiff was a wireless customer of T-Mobile, and had placed an additional level of security onto his account through means of a PIN.

61. At that time, Plaintiff was holding cryptocurrency for personal use and investment on Coinbase – a digital currency wallet and online platform to transfer and store digital currency – using Coinbase's application on Plaintiff's mobile phone, as well as on his computer.

⁸ See, e.g., <https://www.t-mobile.com/privacy-center/education-and-resources/cpni>.

62. Plaintiff entrusted his sensitive private information, including, but not limited to, regarding his cryptocurrency holdings, to T-Mobile and reasonably relied on T-Mobile's assurances of and its stated compliance with applicable laws, including (but not limited to) the FCA.

63. Upon information and belief, including that ultimately provided by T-Mobile, on or around July 5th, 2020, unknown individual(s) visited a T-Mobile store in or around Miami, Florida, where T-Mobile agents allowed and provided that individual(s) unauthorized access to Plaintiff's account and SIM data, including CPI and CPNI. Plaintiff's data was then transferred (or "ported") to another electronic device, and used to access Plaintiff's information and telecommunications service.

64. Upon information and belief, it is also possible that on or around the evening of July 5th, 2020, an unknown individual working for or on behalf of T-Mobile gained unauthorized access to Plaintiff's account and SIM data, including CPI and CPNI. Said individual then transferred Plaintiff's account to another electronic device overnight, using it to access Plaintiff's information and telecommunications services, before transferring the account back to Plaintiff's phone before he awoke in an effort to remain undetected.

65. In other words, Plaintiff was a victim of a SIM-swap that was, if not entirely perpetrated by, then at the very least effectuated and facilitated by T-Mobile and its employees.

66. Plaintiff did not authorize Defendant or anyone else to use, disclose, share, or access his CPI and CPNI that was maintained by T-Mobile.

67. To the contrary, Plaintiff had an objectively reasonable expectation and a fundamental right to conduct his personal activities without observation, intrusion or interference.

68. Therefore, any use, disclosure or access to Plaintiff's account or CPI and CPNI on or around July 5, 2020 was unauthorized and unlawful.

69. As a result of this SIM-swap, Defendant transferred control of Mr. Harris' phone number to a device under the control of the unknown party.

70. Based on T-Mobile's actions, the unknown party was able to bypass the two-factor authentication (also known as "2FA") security measures that Plaintiff had put in place – based on T-Mobile's representations that 2FA would protect Plaintiff's information – thereby compromising Plaintiff's personal, business and financial accounts.

71. On or about July 5th, 2020, using Plaintiff's credentials obtained from T-Mobile, the unknown party stole approximately 1.63151657 bitcoin ("BTC"), with a current estimated value in excess of \$55,000, from Plaintiff's online cryptocurrency wallet with Coinbase.

72. The transfers and login attempts were made overnight while Plaintiff slept. When he awoke in the morning and checked his phone, he did not have any service. After rebooting his phone, service resumed.

73. Upon checking his email account (whose password had been changed), Plaintiff saw a lot of overnight emails indicating that his accounts had been accessed at approximately 2 a.m. EST.

74. Unfortunately, by the time Plaintiff was able to regain access to his account on Coinbase, his digital wallet had been emptied.

75. Later, when Plaintiff was able to communicate with Coinbase support, he discovered that "on July 5th your Coinbase password was reset via email from a Windows 10 device and the IP address 89.187.173.133. Shortly after your password was reset, your account was accessed via the Windows 10 device by entering the newly created password, a 2-step

verification SMS code sent to your verified mobile number, and completing the new device confirmation requirement via email.” His Coinbase account had been completely emptied, with funds transferred to an unknown third-party account.

76. Plaintiff contacted T-Mobile support regarding suspicious activity and charges on his account on or around July 6, 2020. At no point during that phone call was Plaintiff advised that he may have been the victim of a SIM-swap attack, or that Defendant had authorized the transferring of Plaintiff’s CPI and CPNI to a third party.

77. T-Mobile indicated to Plaintiff that someone had requested changes to his account at a store location. When Plaintiff told T-Mobile he had not requested any changes to his account, they told him to not worry about any charges made to his account, and that they would be removed.

78. T-Mobile would not indicate to Plaintiff that he was the subject of an unauthorized SIM-swap until over two months later, after Plaintiff had sent a letter of complaint to T-Mobile.

79. Hence, it was not just T-Mobile’s act of providing the unknown hacker(s) with access to Plaintiff’s account without adhering to T-Mobile’s security protocols, but also T-Mobile’s failure to timely and properly diagnose the cause of Plaintiff’s service interruption, as well as to notify Plaintiff, that allowed the cryptocurrency theft to occur and persist.

80. Plaintiff alerted local and federal law enforcement authorities of this development and, to the best of Plaintiff’s knowledge, information and belief, the investigation into the identity of the third parties who gained access to Plaintiff’s SIM data from T-Mobile is ongoing.

81. According to T-Mobile, multiple investigations were undertaken internally to uncover the facts surrounding this theft, including information on who at T-Mobile participated in these actions.

82. To the best of Plaintiff's knowledge, information and belief, T-Mobile knows the identity of those individuals working for or on behalf of T-Mobile who participated in the actions complained of herein.

83. On or about May 3, 2021 Plaintiff requested information from T-Mobile pursuant to the Fair and Accurate Credit Transactions Act ("FACTA"), which requires a response within 30 days, regarding his account and these investigations. No response was ever forthcoming from T-Mobile, despite their assurances to the contrary that such information would be shared with Plaintiff.

84. Upon information and belief, T-Mobile, despite a legal obligation to do so, abjectly failed in its duty to safeguard its customers' personal and financial information by providing unauthorized access to Plaintiff's CPI and CPNI.

85. Upon information and belief, T-Mobile failed to implement and/or maintain security policies and procedures sufficient to protect the unauthorized access to Plaintiff's CPI and CPNI.

86. Upon information and belief, T-Mobile failed to properly train and supervise its employees to prevent the unauthorized access to Plaintiff's CPI and CPNI.

87. Upon information and belief, T-Mobile could have reasonably foreseen the consequences of failing in its duty to implement, maintain, and execute sufficient security policies and practices to protect the unauthorized access to consumer data, including that of Plaintiff.

88. Upon information and belief, T-Mobile's systems, policies, and procedures allow its officers, agents, and employees to exceed the authorized access to customers' accounts without permission or justification.

89. T-Mobile's actions and inaction demonstrate a reckless disregard for the rights of its customers and those with whom its customers deal (i.e. other foreseeable victims).

90. T-Mobile's actions and inaction also demonstrate a reckless disregard for its obligations, responsibilities and duties under the law.

91. The damage suffered by Plaintiff is directly related to the wrongful conduct of allowing the unauthorized access to Plaintiff's wireless account.

92. Indeed, but for T-Mobile's reckless disregard of its obligations, Plaintiff would not have been damaged.

93. By its procedures, practices and regulations, T-Mobile engages in practices that, taken together, fail to provide reasonable and appropriate security to prevent unauthorized access to its customer wireless accounts, allowing unauthorized persons to be granted access to sensitive customer wireless accounts and data.

94. T-Mobile:

- a. failed to establish or enforce rules sufficient to ensure only authorized persons have access to T-Mobile customer accounts;
- b. failed to establish appropriate rules, policies or procedures for the supervision and control of its officers, agents or employees;
- c. failed to establish or enforce rules, or provide adequate supervision or training sufficient to ensure that all of its employees or agents follow the same policies and procedures. For example, upon information and belief, it is often possible to persuade one of T-Mobile's agents not to apply the stated security policies and allow unauthorized access without providing a PIN;

- d. failed to adequately safeguard and protect its customer wireless accounts, including that of Plaintiff, so unauthorized third parties were able to obtain access to Plaintiff's account(s);
- e. permitted the sharing of and access to user credentials among T-Mobile's agents or employees without a pending request from the customer, thus reducing likely detection of, and accountability for, unauthorized access;
- f. failed to suspend user credentials after a certain number of unsuccessful access attempts;
- g. failed to adequately train and supervise its agents and employees, allowing its agents or employees, without authorization or approval, to unilaterally access and make changes to customer accounts as if the customer had so authorized;
- h. allowed porting out of phone numbers without properly confirming that the request was coming from legitimate customers;
- i. lacked proper monitoring solutions and thus failed to monitor its systems for the presence of unauthorized access in a manner that would enable T-Mobile to detect the intrusion, so that the breach of security and diversion of customer information was able to occur in the Plaintiff's situation and continued until after his virtual currency account was compromised;
- j. failed to implement simple, low-cost, and readily available defenses to identity thieves, such as delaying transfers from accounts on which the password was recently changed or simply delaying transfers from accounts to allow for additional verifications from the customer; and

- k. failed to build adequate internal tools to help protect the customers; and against hackers and account takeovers, including protection from phone porting and wrongdoing by its own agents or employees acting on their behalf or on behalf of or at the request of a third party.

95. As such, T-Mobile's security measures were entirely inadequate to protect its customers, including Plaintiff.

D. CAUSES OF ACTION

Count I Violation(s) of the FCA

96. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

97. The FCA regulates interstate telecommunications carriers, including T-Mobile.

98. T-Mobile is a "common carrier" or a "telecommunications carrier" engaged in interstate commerce by wire for the purpose of furnishing communication services within the meaning of Section 201(a) of the FCA. See 47 U.S.C. §201(a).

99. As a "common carrier", T-Mobile is subject to the substantive requirements of Sections 201 through 222 of the FCA. See 47 U.S.C. §§201-222.

100. Under Section 201(b) of the FCA, common carriers may implement only those practices, classifications, and regulations that are "just and reasonable" and practices that are "unjust or unreasonable" are unlawful.

101. Section 206 of the FCA, entitled "Carriers' liability for damages" provides:

In case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of

this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case.

102. Section 207 of the FCA, entitled "Recovery of damages" further provides:

Any person claiming to be damaged by any common carrier subject to the provisions of this chapter may either make complaint to the [FCC] as hereinafter provided for, or may bring suit for the recovery of the damages for which such common carrier may be liable under the provisions of this chapter, in any district court of the United States of competent jurisdiction; but such person shall not have the right to pursue both remedies.

103. Section 222(a) of the FCA explicitly requires that a telecommunications carrier protect its customers' CPI. See 47 U.S.C. §222(a).

104. Additionally, Section 222(c) of the FCA explicitly requires that telecommunications carriers protect its customers' CPNI. See 47 U.S.C. §222(c).

105. According to the CPNI Rules:

Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated contact, online account access, or an in-store visit.

...

In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.⁹

106. T-Mobile violated its duties under Section 222 of the FCA by failing to protect Plaintiff's CPI and CPNI by using, disclosing, or permitting access to Plaintiff's CPI and CPNI

⁹ 47 C.F.R. §64.2010(a), (d). For purposes of the CPNI Rules, the term "customer" means "[a] person...to which the telecommunications carrier is currently providing service," while the term "valid photo ID" means "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired." 47 C.F.R. §64.2004(f), (r).

without the consent, notice, and/or legal authorization of Plaintiff as required by the FCA, in that upon information and belief:

- a. during an in-store visit, perhaps in Miami, Florida, Plaintiff's CPI and CPNI were disclosed to someone other than Plaintiff by an agent of Defendant;
- b. during an in-store visit, Plaintiff's CPI and CPNI were disclosed to someone, who was not properly authenticated by Defendant;
- c. during an in-store visit, Plaintiff's CPI and CPNI were disclosed to someone, who did not first present a valid photo ID to Defendant; and/or
- d. during an in-store visit, Plaintiff's CPI and CPNI were disclosed to someone, who did not match any of Plaintiff's account information that T-Mobile was aware of, including (but not limited to) the fact that Plaintiff's account was opened and operating out of the Philadelphia area (not Miami).

107. As alleged herein, T-Mobile failed to protect the confidentiality of Plaintiff's CPI and CPNI when it disclosed Plaintiff's CPNI and CPI to third-parties without Plaintiff's authorization or permission.

108. T-Mobile's conduct, as alleged herein, constitute knowing violations of the FCA, including sections 201(b) and 222, as well as the CPNI Rules.

109. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, or its officers, employees, agents, or any other persons acting for or on behalf of T-Mobile.

110. T-Mobile's violation of the FCA allowed unauthorized parties to impersonate Plaintiff in transactions with others.

111. T-Mobile violated the FCA, including Section 222, by allowing an unauthorized party to access Plaintiff's CPI and CPNI, resulting in, *inter alia*, Plaintiff's loss of his possessions, including 1.63151657 BTC, with a current estimated value in excess of \$55,000.

112. As a direct consequence of T-Mobile's violations of the FCA, Plaintiff has been damaged through the loss of his property, namely 1.63151657 BTC.

113. Had T-Mobile not allowed the unauthorized access to Plaintiff's account, Plaintiff would not have suffered this loss.

114. T-Mobile, by its inadequate procedures, practices, and regulations, engages in practices which, when taken together:

- a. fail to provide reasonable, appropriate, and sufficient security to prevent unauthorized access to its customers' wireless accounts;
- b. allow unauthorized persons to be authenticated; and
- c. grant access to sensitive customer account information.

115. In particular, T-Mobile failed to establish and implement reasonable policies, procedures and safeguards governing the creation, access, and authentication of user credentials to access customers' accounts, creating an unreasonable risk of unauthorized access.

116. As such, in violation of the FCA, T-Mobile has failed to ensure that only authorized persons have access to customer account data and that customers' CPI and CPNI are secure.

117. Among other things, T-Mobile:

- a. failed to establish and enforce rules and procedures sufficient to ensure only authorized persons have access to T-Mobile customer accounts, including that of Plaintiff;

- b. failed to establish appropriate rules, policies and procedures for the supervision and control of its officers, agents and employees;
- c. failed to establish and enforce rules and procedures, or provide adequate supervision or training sufficient to ensure that its employees and agents follow such rules and procedures, to restrict access by unauthorized persons;
- d. failed to establish and enforce rules and procedures to ensure T-Mobile's employees and agents adhere to the security instructions of customers with regard to accessing customers' accounts, including that of Plaintiff;
- e. failed to adequately safeguard and protect its customers' wireless accounts;
- f. permitted the sharing of and access to user credentials among T-Mobile's agents or employees without a pending request from the customer, reducing the likely detection of and accountability for unauthorized access;
- g. failed to appropriately supervise employees and agents, who granted unauthorized access to customers' accounts, including that of Plaintiff;
- h. failed to adequately train and supervise its employees, officers and agents to prevent the unauthorized access to customer accounts;
- i. failed to prevent the ability of employees, officers and agents to access and make changes to customer accounts without specific customer authorization;
- j. allowed "porting out" of cell phone numbers without properly confirming that the request was coming from legitimate customers;
- k. lacked proper monitoring and, therefore, failed to monitor its systems for the presence of unauthorized access in a manner that would allow T-Mobile to

detect intrusions, breaches of security, and unauthorized access to customer information;

- l. failed to implement and maintain readily available best practices to safeguard customer information (and indeed, seemed to suggest such practices were only available to those customers who “paid for” the privilege of having their information secured);
- m. failed to timely diagnose and determine the cause of Plaintiff’s service interruption;
- n. failed to timely notify Plaintiff of the cause of Plaintiff’s service interruption; and
- o. failed to implement and maintain internal controls to help protect against account takeovers and SIM-swaps by unauthorized persons.

118. The inadequate security measures, policies and safeguards employed by T-Mobile created a foreseeable and unreasonable risk of unauthorized access to the accounts of its customers, including that of Plaintiff.

119. Upon information and belief, T-Mobile has been long aware of its inadequate security measures, policies and safeguards, and nevertheless, induced customers into believing that its systems were secure and compliant with applicable law.

120. T-Mobile, despite knowing the risks associated with unauthorized access to customer accounts, failed to utilize reasonable and available methods to prevent or limit such unauthorized access.

121. T-Mobile failed in its duty to protect and safeguard customer information and data pursuant to federal law.

122. Had T-Mobile implemented appropriate and reasonable security measures, Plaintiff would not have been damaged.

123. In sum, Defendant's security measures were entirely inadequate to prevent the foreseeable damage caused to Plaintiff.

Count II
Negligence

124. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

125. T-Mobile owes a duty of care to its customers to ensure the privacy and confidentiality of CPI and CPNI during its provision of wireless carrier services, as required by both federal and state law.

126. By allowing unauthorized access to the personal and confidential information of legitimate T-Mobile customers, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

127. By failing to timely and properly diagnose the cause of Plaintiff's service interruption, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

128. But for the inadequate security protocols, practices, and procedures employed by T-Mobile in protecting customer data, including Plaintiff's private and confidential information, Plaintiff would not have suffered any damage.

129. But for the inadequate protocols, practices, and procedures employed by T-Mobile in diagnosing the causes of customers' service interruptions, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

130. But for those intentional actions and/or inaction of Defendant and its agents, Plaintiff would not have suffered damages.

131. And but for T-Mobile's inability to quickly and effectively diagnose and/or determine that Plaintiff's account was compromised by a SIM-swap – a fact that T-Mobile should have known – Plaintiff would not have suffered damages.

132. Plaintiff has been damaged through the loss of his property, namely 1.63151657 BTC, with a current estimated value in excess of \$55,000.

Count III
Negligent Hiring, Retention and Supervision

133. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

134. At all material times herein, T-Mobile's agents, officers, and employees, including, but not limited to, those directly or indirectly responsible for or involved in allowing unauthorized access to Plaintiff's confidential and proprietary account information, were under T-Mobile's direct supervision and control.

135. Upon information and belief, T-Mobile negligently hired, retained, controlled, trained and supervised the officers, agents and employees under its control, or knew or should have known that such officers, agents and employees could allow unauthorized access to customer accounts, including that of Plaintiff.

136. Upon information and belief, T-Mobile negligently failed to implement systems and procedures necessary to prevent its officers, agents and employees from allowing or obtaining unauthorized access to customer accounts, including that of Plaintiff.

137. Upon information and belief, T-Mobile's negligent hiring, retention, control, training and supervision allowed the unauthorized access to customers' accounts resulting in damage to T-Mobile customers and foreseeable victims in the public at large, including Plaintiff.

138. Given T-Mobile's experience with account takeover and SIM-swap attacks (including some perpetrated and/or assisted by Defendant's own employees, officers or agents), T-Mobile's failure to exercise reasonable care in screening, supervising, and controlling its officers, agents and employees was a breach of its duty to its customers, including Plaintiff.

139. T-Mobile's duty to its customers and foreseeable victims to protect its customers' data from unauthorized access is required by federal and state law.

140. It was entirely foreseeable to T-Mobile that unauthorized persons would attempt to gain unauthorized access to T-Mobile customers' data and, despite this, T-Mobile failed to implement sufficient safeguards and procedures to prevent its officers, agents and employees from granting or obtaining such unauthorized access.

141. Upon information and belief, T-Mobile engaged in the acts alleged herein and/or condoned, permitted, authorized and/or ratified the conduct of its officers, agents and employees.

142. As a direct consequence of T-Mobile's negligent hiring, retention, control and supervision of its officers, agents and employees, who enabled or obtained the unauthorized access to Plaintiff's account, Plaintiff was damaged through the loss of his property, namely 1.63151657 BTC, with a current estimated value in excess of \$55,000.

Count IV
Gross Negligence

143. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

144. T-Mobile, as required by federal and state law, owed Plaintiff a duty to properly handle and safeguard Plaintiff's CPI and CPNI and access to his account.

145. T-Mobile was required to ensure its compliance with federal law and to protect the confidentiality of its customers' account data, including that of Plaintiff.

146. Upon information and belief, T-Mobile willfully disregarded and/or showed reckless indifference to its duties under federal and state law to T-Mobile customers and to foreseeable victims of T-Mobile's wrongful acts.

147. Having superior knowledge of prior account takeover attacks on T-Mobile customers' data and having the ability to employ internal systems, procedures, and safeguards to prevent such attacks, T-Mobile nevertheless failed:

- a. to institute appropriate controls to prevent unauthorized access to customers' accounts;
- b. utilized authentication systems it knew or should have known were vulnerable to account takeover attacks;
- c. willfully disregarded the best practices of the industry in failing to implement systems to thwart such attacks; and
- d. failed to appropriately hire, retain, supervise, train and control those officers, agents and employees who could grant or obtain unauthorized access to customer account data.

148. T-Mobile's policies, procedures and safeguards were completely ineffective and inadequate to prevent the unauthorized access to its customers' data, notwithstanding the requirements of the CFA.

149. T-Mobile's actions as alleged herein, in the face of an abundance of attention by the media and government regulators, as well as multiple pieces of litigation filed against them, evidence a carelessness that can only be characterized as a complete disregard for the rights of its customers and the foreseeable victims of its inadequate data security measures.

150. As a consequence of T-Mobile's gross negligence, Plaintiff has been damaged through the loss of his property, namely 1.63151657 BTC, with a current estimated value in excess of \$55,000.

Count V
Violation of the Stored Communications Act

151. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

152. Under the Stored Communications Act ("SCA"), 18 U.S.C. §2701 *et seq.*, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. §2702(a)(1).

153. Section 2702(a)(2) of the SCA further states:

[A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service (A) on behalf of, and received by means of electronic transmission from (or created by means of electronic transmission from), a subscriber or customer of such service; [or] (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for the purposes of providing any services other than storage or computer processing....

154. Although the SCA contains several exceptions to the prohibitions set forth in Sections 2702(a)(1) and (2), none of them are applicable to the circumstances at issue in this case.

155. The SCA creates a private right of action for those “aggrieved by any violation” of its provisions. 18 U.S.C. §2707(a).

156. The conduct of T-Mobile and Does 1-10, as alleged herein, constitutes a knowing and/or intentional violation of the SCA’s Section 2702(a).

157. Plaintiff has been “aggrieved” by the conduct of T-Mobile and Does 1-10, as alleged herein, in that Plaintiff’s property has been stolen, namely 1.63151657 BTC, with a current estimated value in excess of \$55,000.

158. Pursuant to the applicable provisions of the SCA, Plaintiff is entitled to actual and statutory damages, as well as reasonable attorneys’ fees and costs. See 18 U.S.C. §2702(c).

Count VI
Violation of the Wiretapping and Electronic Surveillance Control Act

159. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

160. Under Section 5742(a)(1) of the Wiretapping and Electronic Surveillance Control Act (“WESCA”), 18 Pa.C.S. §5701 *et seq.*:

A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service...[o]n behalf of, and received by means of electronic transmission from, or created by means of electronic transmission from, a subscriber or customer of the service [or] [s]olely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.¹⁰

161. Under Section 5742(a)(2) of the WESCA:

A person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of

¹⁰ 18 Pa.C.S. §5742(a)(1)(i), (ii).

any communication which is carried or maintained on that service...[o]n behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service [or] [s]olely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

162. Under Section 5742(a)(3) of the WESCA, “[a] person or entity providing an electronic communication service or remote computing service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to, or customer of, the service.” 18 Pa. C.S. §5742(a)(3).

163. Although WESCA contains several exceptions to the prohibitions set forth in Section 5742(a), none of them are applicable to the circumstances at issue in this case. See 18 Pa.C.S. §5742(b), (c), (c.1).

164. WESCA creates a private right of action for those “aggrieved by any violation” of its provisions. See 18 Pa.C.S. §5747.

165. The conduct of T-Mobile and Does 1-10, as alleged herein, constitute knowing and/or intentional violation(s) of WESCA’s Section 5742(a).

166. Plaintiff has been “aggrieved” by the conduct of T-Mobile and Does 1-10, as alleged herein, in that Plaintiff has lost his property, namely 1.63151657 BTC, with a current estimated value in excess of \$55,000.

167. Pursuant to the applicable provisions of WESCA, Plaintiff is entitled to actual and statutory damages, as well as reasonable attorneys’ fees and costs. See 18 Pa.C.S. §5747(c).

Count VII

Violation of the Unfair Trade Practices and Consumer Protection Law

168. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

169. The Unfair Trade Practices and Consumer Protection Law (“UTPCPL”), 73 P.S. §201-1, *et seq.*, provides that “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce...are hereby declared unlawful.” 73 P.S. §201-3.

170. Section 201-2(4) of the UTPCPL defines “unfair or deceptive acts or practices” to include the following conduct:

- a. representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another;
- b. failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to, or after a contract for the purchase of goods or services is made; and
- c. engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding.¹¹

171. T-Mobile’s acts as alleged herein, including (but not limited to) its sales and marketing representations about its level of data security and confidentiality and the measures T-Mobile employs to keep customers’ data secure, induced customers to trade with T-Mobile notwithstanding T-Mobile’s knowledge that its security protocols and procedures were inadequate to prevent unauthorized access to customers’ CPI and CPNI.

172. Plaintiff justifiably relied on these sales and marketing representations.

¹¹ See 73 Pa. C.S. §201-2(4)(vii), (xiv), and (xvii).

173. T-Mobile's actions, as alleged herein, violated federal and state law, particularly those related to the safeguarding of customers' CPI and CPNI, and such violations are violations of the above-referenced provisions of the UTPCPL.

174. Given T-Mobile's superior knowledge of its systems, procedures and practices, coupled with its experience with past breaches of data security (and specifically "SIM-swaps"), Plaintiff was a foreseeable victim of the violative acts of T-Mobile.

175. By allowing unauthorized access to Plaintiff's confidential and proprietary information, T-Mobile facilitated unauthorized third parties to prey upon innocent victims like Plaintiff.

176. By failing to timely and properly diagnose the cause of Plaintiff's service interruption, or to notify him of the same, T-Mobile facilitated unauthorized third parties to access Plaintiff's confidential and proprietary information and to use said information to steal Plaintiff's property.

177. Had T-Mobile accurately represented the nature of its security measures, or lack thereof, Plaintiff would not have become T-Mobile's customer and would not have been damaged by those who gained unauthorized access to his CPI and CPNI from T-Mobile.

178. Therefore, T-Mobile has violated the above-referenced provisions of 73 Pa.C.S. §201-2(4).

179. Section 201-9.2(a) of the UTPCPL authorizes a private cause of action for any person "who purchases or leases goods or services primarily for personal, family or household purposes." 73 P.S. §201-9.2(a).

180. UTPCPL also authorizes the Court, in its discretion, to award up to three (3) times the actual damages sustained for its violations, as well as attorneys' fees.

181. Plaintiff has suffered, and will continue to suffer damages due to the conduct of T-Mobile, as set forth herein.

Count VII
Violation of the Computer Fraud and Abuse Act (CFAA)

182. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

183. The CFAA governs those who intentionally access computers without authorization or who intentionally exceed authorized access and as a result of such conduct, cause damage and loss.

184. As set forth in the CFAA, the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [*sic*] is not entitled so to obtain or alter.” 18 U.S.C. §1030(e)(6).

185. As alleged herein, a SIM-swap attack requires the intentional access to customer computer data by T-Mobile which exceeds its authority, and which conduct has caused damage and loss.

186. T-Mobile is subject to the provisions of the CFAA.

187. T-Mobile’s conduct, as alleged herein, constitutes a knowing violation of the CFAA.

188. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, agents or any other person acting for or on behalf of T-Mobile.

189. T-Mobile violated its duty under the CFAA by exceeding its authority to access the computer data and breach the confidentiality of the proprietary information of Plaintiff by using, disclosing, or permitting access to Plaintiff’s CPI and/or CPNI without the consent, notice and/or legal authorization of Plaintiff as required by the CFAA.

190. Section 1030(g) of the CFAA provides:

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involved 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage....

191. Plaintiff alleged he has suffered damages which exceed the threshold of \$5,000.00 as required by Section 1030(c)(4)(A)(i)(I) of the CFAA.

192. Plaintiff alleged T-Mobile's unlawful conduct has caused damages which exceed \$150,000.00.

193. Plaintiff has brought this claim within two (2) years of the date of discovery of the damage pursuant to Section 1030(g) of the CFAA.

194. Upon information and belief, T-Mobile's conduct as alleged herein constitutes a violation of Section (a)(5)(A) of the CFAA.

195. Upon information and belief, T-Mobile's conduct as alleged herein may constitute an intentional violation of Section (a)(5)(C) of the CFAA.

196. As a direct consequence of T-Mobile's violations of the CFAA, Plaintiff has been damaged as set forth throughout this Complaint, plus fees and costs, including reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that the Court enter judgment in his favor and against Defendants, and for the following:

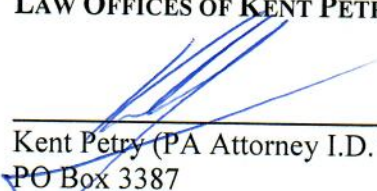
- A. Judgment for Plaintiff on all counts;
- B. Actual damages;
- C. Statutory damages;
- D. Treble damages;
- E. Punitive damages;
- F. Replacement of his property;
- G. Attorneys' fees and costs;
- H. Prejudgment interest; and
- I. Such other relief as this Honorable Court shall deem just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury as to all issues so triable.

Respectfully Submitted,

LAW OFFICES OF KENT PETRY


Kent Petry (PA Attorney I.D. No. 207659)
PO Box 3387
Warminster, PA 18974
(215) 322-1084

Attorney for Plaintiff

Dated: July 6, 2021